UNIVERSITÀ DEGLI STUDI DI MILANO
Ufficio Cert e Gestione Incidenti
Settore Cybersecurity – Direzione ICT

Avviso di sicurezza del 8/03/2024

Segnalazione di campagne malevole con impersonificazione di un Direttore di Dipartimento

Gent.Utenti,

pubblichiamo il presente avviso per segnalarvi la presenza di campagne malevole in atto in queste ore con l'obbiettivo di sottrarre fondi attraverso l'impersonificazione di un Direttore di Dipartimento. In fondo a questo documento potete trovare alcune schermate di esempio.

La campagna solitamente parte con una mail generica di richiesta di supporto inviata da un account non istituzionale, es. Gmail, che mima un account personale del Direttore di un Dipartimento, es. *mario.rossi.unimi.it @ gmail.com* oppure *mario.rossi234 @ gmail.com*. Se la vittima risponde a questo primo messaggio, la conversazione prosegue con una richiesta di un qualche tipo di bonifico motivata dall'urgenza del bonifico e dall'impossibilità di eseguirlo personalmente perché in riunione o fuori sede o qualche altro impedimento.

Questo tipo di attacco per sua natura è pressoché impossibile da identificare in maniera automatica e quindi richiedono particolare attenzione da parte di tutti gli utenti dell'Ateneo. Qualora riceviate nella INBOX uno di questi messaggi, vi chiediamo di inoltrare la mail malevola come allegato a sicurezza@unimi.it prima di cancellarla; sul portale istituzionale potete trovare una guida su come allegare le mail:

LaStatale@Work → Servizi per tutti → Sicurezza informatica e protezione dei dati personali
→ Regolamenti, istruzioni e linee guida
→ Guide ed indicazioni utili per tutti (studenti, personale docente e non docente)
→ come inoltrare una mail come allegato
https://work.unimi.it/filepub/sicurezza_ict/DICT_IO_ComeAllegareMail_rev.2.2_17062021.pdf

Ricordiamo infine alcune buone prassi utili ad aumentare la propria sicurezza informatica e a identificare questo genere di attacchi:

- Se possibile, usare solo canali istituzionali per le attività istituzionali: mail istituzionale, interno telefonico, cellulare d'ufficio, servizi di Ateneo per il trasferimento di file ed informazioni.
- Verificare sempre richieste anomale, specie se di carattere finanziario, attraverso un altro canale di comunicazione, possibilmente istituzionale: chiamata vocale, colleghi, interno telefonico.
- In caso di dubbio potete inoltrare le mail sospette come allegato a sicurezza@unimi.it per un ulteriore controllo; consultate periodicamente gli Avvisi di Sicurezza Informatica del Portale di Ateneo per restare aggiornati: https://work.unimi.it/servizi/security_gdpr/118606.htm

Grazie per la collaborazione.

I più cordiali saluti.

Massimo Marchi
Ufficio Cert e Gestione Incidenti
Settore Cybersecurity – Direzione ICT
Universita' degli Studi di Milano - Via Giuseppe Colombo n. 46 - 20133 Milano

Figura 1: esempio di conversazione malevola

Da: C Maria maria unimi.it@gmail.com
Oggetto: Re:
Data: 22 aprile 2021 12:04
A: @unimi.it

CT

Grazie per la tua risposta, per favore sono in riunione in questo momento, ecco perché ti sto contattando tramite qui Avrei dovuto chiamarti ma il telefono non può essere usato durante la riunione Non so quando la riunione sarà in tondo su e voglio che tu mi aiuti su qualcosa di molto importante subito se c'è qualche negozio di alimentari vicino a te

prof. C Maria

Director
department of
offices.Via Festa del Perdono, 7
20122 MILAN (MI)
UNIVERSITY OF MILAN

On Thu, 22 Apr 2021, 10:54 am @unimi.it> wrote:
Ciao,
Sto entrando in udienza di discussione. Temo lunga. Appena termino ti chiamo.

> Il giorno 22 apr 2021, alle ore 11:42, C Maria <maria unimi.it@gmail.com> ha scritto:
>
> Ciao sei disponibile?
> Per favore, ho bisogno urgentemente della tua assistenza
>
> prof. Maria
>
> Director
> department of
> offices.Via Festa del Perdono, 7
> 20122 MILAN (MI)
> UNIVERSITY OF MILAN

Figura 2: esempio di conversazione malevola